

Professional Services - Compliance

I/T Security Audits

Based on ISO and Regulatory Standards, xDefenders works with clients to interview employees, I/T staff and others, to determine if published security policies are being followed. Essentially, comparing policy with procedures and noting where there are "gaps". A detailed checklist is filled-out and a report is written and reviewed with the client. An audit will review the following business areas:

◆ Web Application Security

We will audit your key web applications and provide you with a report that will detail all remediation needed to secure the applications. We use a number of the industry's best tools. These tools can be run remotely and provide information on a number of known exploits including:

- Cookie poisoning - Identity Theft
- Hidden field manipulation - eShoptlifting
- Parameter tampering - Fraud
- Buffer overflow - Closure of business
- Cross-Site scripting - Hijacking/Breach of trust
- Manipulation of SQL statements
- Backdoor and Debug Options - Trespassing
- Forceful browsing - Breaking and Entering
- Stealth commanding - Concealed Weapons
- 3rd party manipulation - Debilitating a site
- Known vulnerabilities - Taking control of a site

◆ Database Access and Security Controls

Many applications that reside on top of Oracle, Sybase, DB2, MS/SQL or MySQL rely on the security attributes of the database to secure, control and backup the data. Understanding this concept and Data Base Administrator (DBA) processes and tools is essential to auditing a database and the applications that utilize it. We look for and document the relationship between application and database and the standalone security of the database itself.

- Log-On Procedures,
- Password administration and management
- User Identification, Authentication and Administration
- Use of system utilities

◆ Operating System Access Control

- Password Administration and Management
- User Identification, Authentication, Admin.
- Use of System Utilities
- Terminal Time-out
- Limitation of Connection Time
- Terminal Log-On Procedures
- Peripheral Administration

◆ Security of System Files and Servers

- Control of operational software
- Protection of system data and files
- Access control to program source library
- Connectivity and Interconnected network
- Network Access
- Trust relationships
- Server Logical Security
- Penetration detection
- Violation investigation and monitoring
- Virus Protection

◆ Housekeeping

- Management of Logs
- Back-up Procedures
- Fault Logging
- Problem Reporting and Administration

◆ Security Gap Analysis

- Firewall configuration
- Router and switch configuration
- Operating system vulnerabilities
- Virus protection methodologies
- Application vulnerabilities
- Remote access facilities and VPNs
- Monitoring & intrusion detection systems



xDefenders, inc.
1100 Pittsford Victor Rd., Pittsford, NY 14534
(585) 385-2770 www.xDefenders.com



**Certified Information System
Security Professionals (CISSP)**

**Personal, Professional Service
Best-of-Breed and Best-Value Solutions
Satisfaction Guaranteed**

Security Focused:

We help organizations comply with Information Security Regulations, Privacy Laws, and Best Security Practices by protecting their applications, systems, and networks with affordable solutions and personalized, professional service.

Security Services:

xDefenders is an experienced team of information security professionals focused on helping organizations protect the confidentiality, integrity, and availability of their information assets. We employ a "Defense-In-Depth" approach to security that recognizes that technology is only part of the solution. People, policies, and practices are important elements that help mitigate risk and must be addressed in the solution. Professional, Managed and Hosted Security Services include:

Vulnerability & Risk Assessments
I/T Security Audits
Security Policies & Awareness Training
(BCP) Business Continuity Planning

(IPS) Intrusion Prevention Systems
(IDS) Intrusion Detection Systems
Secure and Archived Mail
Managed Security Services 24x7

Credentials:

- ISO, HIPAA, PCI, Homeland Security, NYS Security Policy Standards
- GLBA, NCUA, FFIEC—Financial Industry Security Rules and Regulations
- CISSP—Certified Information Security System Professionals
- CERT—Computer Emergency Response Center
- CIS—Center for Internet Security benchmarks
- ZixCorp MSSP Partner and Cisco Security Partner
- Vender Certifications – Symantec, Checkpoint, Sun, Microsoft
- Modern and up-to-date security tool-kits and techniques

History:

Founded in 2003, xDefenders has focused exclusively on Information Security and the needs of business. We have "Enterprise" experience with systems, networking, web application development, and proven methodologies. xDefenders has a large client base throughout the USA. The Company was acquired by Synergy Global Solutions, a value-added reseller, in April of 2007. Synergy has a strong regional presence in Upstate NY with 200+ employees and sales of \$70 million in 2006. See www.Synergy.gs for more information.



www.xDefenders.com 1100 Pittsford Victor Road, Pittsford, NY 14534 (585) 385-2770

Managed Security Services, 24x7

We work as a member of your I/T team, to improve and maintain your security. As your trusted security partner, xDefenders provides affordable choices in the management and monitoring of key security infrastructure and service components.

We manage, monitor Firewalls, Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), and Central System Log Servers to deliver a centralized, integrated security solution. xDefenders follows the SLA and Escalation Plan to insure the safety and availability of your information assets.

Network & Security Operations Centers (NOC and SOC) in Buffalo and Rochester

Our state-of-the-art network and security management-monitoring facilities are staffed **24x7x365**. These are secure data-centers with redundant power and consoles for remote management by our trained staff. Our professionals use Correlation engines to identify faults/attacks and escalate immediately, according to client policy. A Client Portal is available to view alerts and reports.



Our **Standard Defender Services** include remote monitoring, operating system updates, application software support and subscription, timely database updates, administrative support and next day hardware replacement, Monday thru Friday from 8:30 am to 6 pm.

Our **DefenderPro Services** offer management and monitoring services with a rapid response and administrative support, 24 hours per day, 7 days per week, leveraging the NOC and SOC resources. NOC and SOC staff monitor for attacks and escalate response according client policy.



DefenderWall appliances are based on rackable, scalable HP servers. We include all aspects of remote security and system administration, alert monitoring, and hardware maintenance.

DefenderWall®

Managed Security Appliance - applications:

AppDefender: Protect critical Web applications with this “reverse proxy” HTTP/S firewall. This appliance provides NAT, blocks SQL-injections and other malicious attacks.

ESM—Enterprise Syslog Manager: automatically collects **syslog data** from critical systems and network devices. A Daily Over-Threshold Report is produced. A correlation engine (Bacon) provides real-time alerts and escalation. Graphical Web Dashboard. Automatic and manual fine-tuning.

HostDefender: For **Host Intrusion Prevention (HIPS)**, xDefenders will provide a central management console that will allow Host Security Policy to be enforced. Sygate and CSA are the tools we use to detect and deter unacceptable activity. Policy development and tuning included.

NetDefender: The **(IDS) Intrusion Detection System** includes the industry's #1 Snort (signature database), BASE (reporting) and “Bacon” (correlation and escalation engine). With tuning.

MaiDefender®: This policy-based solution will eliminate **SPAM and Viruses** from your email environment. Incorporates Grey-Listing, LDAP integration, Real-Time Black-hole Lists, Scoring Spam Filter, and Virus updates made every 10 minutes from 3 different sources. Mail Server incl.

MonMan: remote management and monitoring of Cisco ASA, Pix, Security Routers and other network devices. Up-time and syslog event data is monitored from our 24x7 SOC. A copy of the device configuration is stored for a fast restore.

SysDefender: Supports a “Test and Patch” security strategy for internal and external **network & system Vulnerabilities**. Over 13,000 tests are performed with vendor remediation advice. This portable appliance reduces your cost of security testing. Reports are based on the PCI Standard and reveal “Risk Levels”. CISSP consulting incl.

WebDefender: Enforce your Acceptable-Use-Policy. This **Web Content Filtering** solution restricts access to undesirable web sites. With web caching, LDAP integration and Group support.

Professional Services - Compliance

Security Consulting

- Best Practices and Best Protections
- Secure Routing, Switching & Firewall Configurations
- Secure Remote Access and Authentication
- High-Availability Configurations
- Intrusion Detection Systems with Incident Response
- Intrusion Prevention Systems

Vulnerability Assessments

This technical risk assessment service is based on the PCI (MasterCard and VISA) standard which includes planned and unplanned penetration tests upon your network and systems to determine their level of *vulnerability*. This will help you determine your level of security risk externally, as well as from within. We take a personal approach to the project and guarantee customer satisfaction.

Our testing plan is comprehensive. It can include:

- Internet and External Networks
- Social Engineering
- Modems and Wireless
- Web Applications and Databases

We classify vulnerabilities – open ports, down-level operating systems, and suspect applications – as **Urgent-Critical-High-Medium-Low Risk**. We do not exploit found vulnerabilities. We produce Management and Technical Reports and our CISSP's will review them with you during an interactive session. Periodic and adhoc testing is recommended and our Subscription Service is offered.

Business Impact Analysis, Continuity Planning

Business Continuity Planning (BCP) is a collection of management processes designed to provide organizational persistence during and following a business disaster. BCP combines a variety of unique skills encompassing project and crisis management involving business resumption and the implementation of continuous availability.

When disaster strikes, a Business Continuity Plan drives and shapes how an organization behaves by defining how resources are used to control and restore order during disaster conditions. This service includes the custom architecture and implementation of a secure, powerful, and reliable method to secure information off-site.

Security Policy Development & Review

A set of security policies is a reflection of the culture of the organization. It needs to be clearly articulated and communicated to employees and business partners. GLBA, HIPAA and Homeland Security Act call for well-constructed and publicized security policies, for banks, healthcare and governmental organizations, respectively.

- Access Authorization
- Access Establishment
- Access Modification
- Data Backup
- Media Controls
- Passwords
- Personnel Security
- Sanctions
- Security Breach Reporting
- Security Breach Response
- Security
- Service Provider
- Termination
- Training
- Workstation Use
- Internet Acceptable Use

Employee Awareness Training

Most organizations are vulnerable to Social Engineering attempts to gain vital knowledge, which can lead to a compromise. xDefenders offer (3) types of Security Training to help clients increase awareness and reduce their risk of compromise. Instructor-led Classroom Training is typically 1 hours in length. Also offered is Web-based Training and a Self-Study Manual.

Information Risk Assessment Service

xDefenders can help assess the level of security you need to design into your applications, systems and networks by following a proven evaluation model. This Information Risk Management Plan compares and considers key information components and helps you assign a security service for data or program segment to be secured, and the costs associated with the desired security service. The selection and use of security measures is then based on an analysis of system performance, cost of hardware, software, and services. The Plan will provide for the adequate protection of all proprietary, confidential, and privileged information assets valuable to your company, from all threats, whether internal or external, deliberate or accidental.



Certified Information System Security Professionals (CISSP)